PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

Appln No. 09/626,699
Docket No. 562492002620

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/08, H04Q 7/38

A1

(11) International Publication Number: WO 00/25475

(43) International Publication Date: 4 May 2000 (04.05.00)

(21) International Application Number: PCT/US99/24522

(22) International Filing Date: 19 October 1999 (19.10.99)

(30) Priority Data:
09/178,192 23 October 1998 (23.10.98) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventor: QUICK, Roy, Franklin, Jr.; 4502 Del Monte Avenue, San Diego, CA 92107 (US).

(74) Agents: OGROD, Gregory, D. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

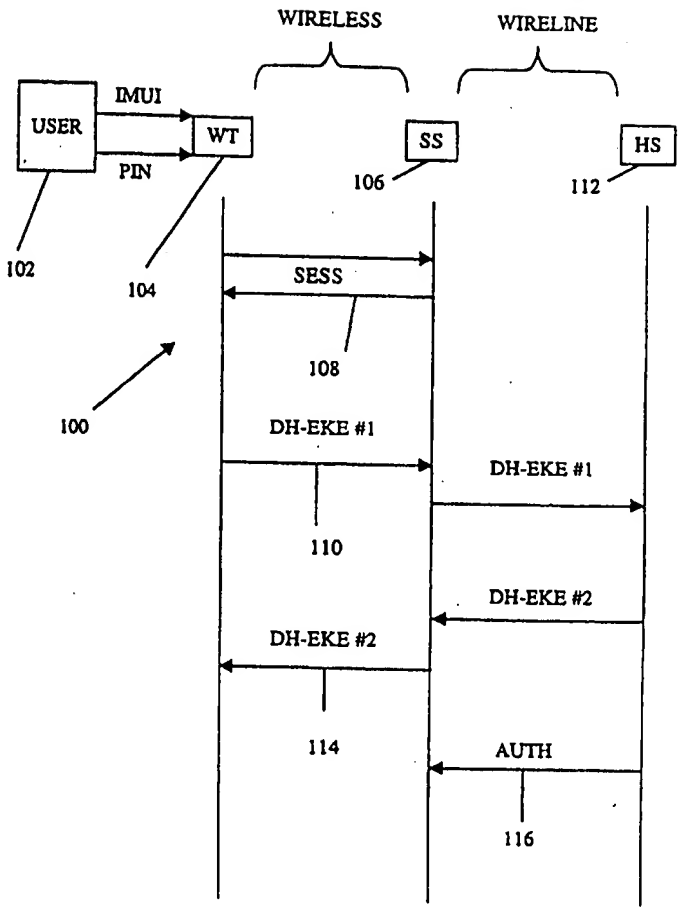
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SUBSCRIPTION PORTABILITY FOR WIRELESS SYSTEMS

(57) Abstract

A short Personal Identification Number (PIN) is used to transfer a subscription for wireless service to a new wireless terminal (104), thereby providing enhanced personal mobility to the subscriber. The transfer is rendered secure by the exchange of Diffie–Hellman Encrypted Key Exchange (DH–EKE) messages (110, 114).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SUBSCRIPTION PORTABILITY FOR WIRELESS SYSTEMS

I. Technical Field

This invention relates to wireless voice and data systems, and has particular relation to allowing a subscriber to move his subscription from one wireless terminal to another. The invention thus provides subscription portability, sometimes also called personal mobility.

II. Background Art

A wireless terminal (portable telephone, laptop computer, etc.) cannot be used as such unless its user has subscribed to a wireless communications service, so that the terminal may use that service to communicate with other terminals, both wireless and wireline. This in turn requires the service provider to register and provision that terminal, that is, to recognize that terminal as being entitled to service and to program the terminal with identification and security information that allows it to access the wireless service.

In the wireless service industry the term "registration" has several meanings. Herein the term "registration" will be used to mean an exchange of the information needed to establish the identity of the user of a terminal and to permit access to wireless services.

This registration may be required in two situations. First, when the terminal is originally purchased, it is not registered to anyone. This situation is referred to as initial provisioning. Second, a subscriber may choose to re-register, that is, to transfer his subscription from one wireless terminal to another. This re-registration might be, for example, from his portable telephone to his laptop computer, or from his regular portable telephone to the portable telephone which he has just rented on a trip to a distant city. This re-registration is referred to as subscription portability.

In early wireless systems such as the analog Advanced Mobile Phone Systems (AMPS), provisioning is performed manually by trained personnel at a terminal distribution site. One of these employees manually registers the terminal with the service provider, typically over the landline telephone. The employee enters information into the terminal through the

keypad, using secret information which the service provider has made available to him/her, and storing the subscription information permanently in the terminal. This arrangement is expensive because the seller must have extensively trained employees at every retail outlet. Furthermore, the process is not secure, since the secret information is readily available to these employees.

One alternative means for dealing with both initial provisioning and subscription portability is to provide to the user a separate, removable device known as a user identification module (UIM). The service provider provisions identity and security information into the UIM before distributing it to the user. When the user inserts the UIM into a terminal, the terminal reads the necessary identity information from the UIM and thereby acquires the identity of the user's subscription. This means is popular in the Global System for Mobiles (GSM) system. Registering the terminal after insertion of the UIM is an over-the-air process, and involves a three-way transfer of information between the module, a base station operated by the service provider (which has a unique identification number), and the wireless terminal itself (which has a unique Electronic Serial Number, or ESN).

This first alternative means is still not entirely satisfactory. It requires an electronic interface between the module and the wireless terminal and this interface adds cost to the terminal. Further, the interface is open to contamination when the UIM is removed and inserted, and consequently may become unreliable with repeated use.

A second alternative means deals with the initial provisioning but not with subscription portability. This second means requires that, when the subscriber first buys a new telephone, the user dials a special number to reach a customer service representative who can determine the credit of the user and can then program the necessary subscription information into the terminal using over the air messages.

This second alternative means is an improvement over the UIM means in that it requires no special interface in the terminal. This second means, however, is also not entirely satisfactory, because the service provider must still have highly skilled personnel in the customer service center to operate the over-the-air programming equipment. The expensive nature of the customer service process prohibits the subscriber from re-registering a telephone which a friend has loaned to him for a day or two.

The purpose of this invention is to provide a method for initial provisioning and subscription portability that does not require skilled

personnel to complete the provisioning and registration process, nor a removable item that the user must physically insert into the terminal.

The procedure described herein requires only that the subscriber enter his/her portable wireless subscription identifier, or user identifier (conventionally, his International Mobile User Identifier, or IMUI) and a password (conventionally, his Personal Identification Number, or PIN) into a wireless terminal. The password may be entered into the terminal in any convenient manner, such as keying a number into a keypad, speaking a phrase (with suitable voice recognition technology) into the microphone, or any other convenient manner. The wireless terminal is then able to contact the service provider using over-the-air signals, obtain necessary subscription information, and automatically reprogram itself – and reprogram the service provider – so that the service provider thereafter recognizes this wireless terminal as being registered to this subscriber. The password must be fairly short – typically four to six digits, as in bank card PINs – because the average subscriber cannot memorize a security code that is sufficiently long (twenty digits or more) to impede a brute-force attack.

It is evident that the password must be protected from compromise during the registration process, otherwise the subscription information would be subject to cloning by fraudulent users who obtain the user identifier and password. Recent advances in cryptography, such as the work of Bellovin and Merritt, cited below, provide techniques for securely verifying that the terminal and wireless network both know the correct password without revealing the password. These techniques also provide means for establishing encryption keys that can be used in the encryption of subscription information exchanged subsequent to the initial password confirmation. The existence of these techniques makes it possible to support registration for initial provisioning and subscription portability without need for removable UIMs nor for customer service intervention.

BRIEF DISCLOSURE OF THE INVENTION

Applicant has developed a subscription which is truly portable from one wireless terminal to another, and which uses passwords which are both short and secure.

Whenever a subscriber wishes to register a terminal to his subscription, he enters his user identifier (conventionally, his International Mobile User Identifier, or IMUI) and his password (conventionally, his

Personal Identification Number, or PIN) into the terminal. The terminal generates a public/private key pair and stores it. This key pair is preferably a Diffie-Hellman (D-H) key pair. It optionally concatenates the public key with a random number, and encrypts the (optionally concatenated) number with the password. Any convenient Secure Key Exchange (SKE) method may be used. Several suitable SKE methods are described in Thomas Wu, "The Secure Remote Password Protocol," *Proc. 1998 Internet Society Network and Distributed System Security Symposium*, San Diego, CA, March 1998, pp. 97-111, http://jafar.stanford.edu/srp/ndss.html, and in David P. Jablon, "Strong Password-Only Authenticated Key Exchange," of Integrity Sciences, Inc., of Westboro, Massachusetts, USA, March 2, 1997, http://world.std.com/~dpj/speke97.html, the disclosures of which are incorporated herein by reference. The Diffie-Hellman Encrypted Key Exchange (DH-EKE) method of Bellovin and Merritt is particularly suitable, and the remaining description of the present invention is made with reference to DH-EKE. See Steven M. Bellovin and Michael Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," in *Proc. IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 72-84, May 1992, the disclosure of which is incorporated herein by reference. Either elliptic curve or exponential groups can be used with this method. The resulting encrypted message is called the DH-EKE message.

The terminal then makes wireless contact with a local serving system and requests registration. This serving system may be the subscriber's home system, but often it is not. In any event, the terminal and the home system must be assured of each other's identities, whether there is no intermediate serving system, one system, or even several. The remainder of this description assumes one intermediate system, but is readily modified to handle none or several. That is, the terminal and the home system will always be the source and destination (or vice versa) of messages, regardless of how many intermediate systems (if any) they have to pass through.

The terminal tells the serving system what the subscriber's home system is, by stating either the full user identifier or enough of the user identifier as is necessary to identify the home system. It also states the DH-EKE message. Preferably, the serving system first provides its D-H public key to the terminal, so that the specifics of who is requesting registration are not sent in the clear. Also preferably, the serving system opens a channel with the terminal to facilitate the registration process.

The serving system sends the DH-EKE message to the home system, which decrypts it with the password. The password is known only to the home system and the subscriber. The home system thereby recovers the subscriber's public key. The home system generates its own D-H public/private key pair and stores it. It then concatenates the newly generated public key with a random number, encrypts the concatenated number with the password using DH-EKE, and transmits this newly generated DH-EKE message back to the terminal. The terminal decrypts it with the password and recovers the home-system public key.

The terminal and the home system are now each in possession of its own private key and the other's public key, both of which are far larger than the password. Each is thus able to generate a common session key using conventional methods. Each is further able to securely use the session key to download a virtual User Identification Module (VUIM) into the terminal, that is, to provide to the terminal, over the air, some or all of the information which otherwise would be obtained from a physical UIM (PUIM) being inserted into the terminal.

Registration may now continue in the conventional fashion, as though a PUIM had been used. Alternatively, registration may be included within the downloading process. This is possible since a terminal with a VUIM already has something which a terminal with a PUIM does not acquire until later, namely, a communications link to (and a shared secret session key with) the home system.

A strength of this method is that the public keys are temporary, and can be replaced on each subsequent registration. Further, each public key is essentially a random number, providing no indication whether an attempted decryption was or was not successful. An off-line dictionary attack therefore fails. The only thing that a dictionary attacker recovers is a collection of possible public keys, none of which has anything to distinguish it from any of the others. There is thus nothing to distinguish a correct guess of the password from an incorrect guess. The follow-on on-line attack must therefore still use the entire dictionary of passwords, and will therefore fail.

This strength may also be viewed as the password being used as a private key in a key exchange procedure, rather than as an encryption key *per se*. It is for this reason that the process is called *Secure* Key Exchange rather than *Encrypted* Key Exchange. It is not necessary that the terminal and home system exchange passwords nor session keys in encrypted form. What is important is that the home system be assured that the terminal

knows the password and has the common session key. It is also important that the password not be discoverable by eavesdroppers while the terminal is demonstrating its identity to the home system. If the password is not included in the message, even in encrypted form, then it is more difficult to be compromised.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows an exchange of DH-EKE messages.

FIG. 2 shows an authentication procedure.

DETAILED DESCRIPTION

FIG. 1 shows an exchange 100 of DH-EKE messages. The user 102 enters the user identifier and password into the wireless terminal 104. The terminal 104 generates a pair of Diffie-Hellman (D-H) private and public keys, and stores them. Optionally, the terminal 104 and the base station of the serving system 106 carry out a separate procedure to establish a local session encryption key SESS 108 to protect the user identifier from interception. The terminal 104 uses the password to encrypt the D-H public key, optionally concatenated with a random number before encryption, then transmits the user identifier (optionally encrypted under the local session key) and the encrypted public key, that is, a first DH-EKE message 110, to the base station of the serving system 106 in a registration request. This request should result in a dedicated channel assignment in order to complete the download procedure efficiently.

The serving system 106 contacts the home system 112 requesting a subscription registration. The home system 112 decrypts the wireless terminal's public key using the password in the subscription record. The home system then creates a private and public D-H key, from which a tentative session key is obtained using the terminal's public key and the home system's private key. The home system then encrypts its own public key, optionally concatenating a random number before encryption, using the password stored in the subscription record and returns it in the form of a second DH-EKE message 114 to the wireless terminal 104 via the serving system 106. The wireless terminal 104 decrypts the home system's public key and creates (hopefully) the same tentative session key, using the home system's public key and its own private key.

FIG. 2 shows an authentication procedure 200 which must follow the DH-EKE exchange. The wireless terminal 104 and home system 112 carry out this procedure to prove that each have the same key. This authentication could be either unilateral (for example, only allowing the home system 112 to authenticate the wireless terminal 104) or bilateral. The bilateral technique has three steps. First, the wireless terminal 104 encrypts a random number C_W and sends the encrypted number $E(C_W)$ 202 to the home system 112. Second, the home system 112 generates its own random number C_H, encrypts (C_W, C_H) and sends the encrypted number $E(C_W, C_H)$ 204 to the wireless terminal 104. Third, the wireless terminal 104 encrypts C_H and sends the encrypted number $E(C_H)$ 206 to the home system 112. A unilateral procedure could, for example, omit the first step, and replace C_W in the second step by a second random number.

The public keys were encrypted by the password, and the authentication consists of three different things being sent in an interlocked manner. Therefore, a man-in-the-middle attacker cannot cause a false acceptance of keys, and cannot know the mutual key without breaking the discrete logarithm or elliptic-curve group. Such breakage is currently considered infeasible if the group size is sufficiently large.

If the home system 112 verifies the session key of the wireless terminal 104, it will transfer the subscription information – that is, all or part of a virtual UIM (VUIM) -- to the serving system 106, in both encrypted form for over-the-air transmission and in unencrypted form for use by the serving system. The session key – or, at least, a first portion of it – can also serve as an authentication key AUTH 116 for subsequent authentications of the terminal 104 in the serving system 106. This has advantages over the current cellular authentication procedures in that the authentication key is created at each registration, and therefore will change randomly from registration to registration. Typically the D-H exchange produces 512 bits of output, which is more than are needed for authentication. As a result, the remainder of the session key, that is, a second portion of it, can serve as a conventional encryption key for subsequent control signal transmissions.

The serving system 106 downloads the encrypted subscription data – the VUIM – to the terminal and makes a registration entry in the Visitor Location Register (VLR). The user is now ready to make calls.

For subsequent system accesses, the user can be assigned a Temporary Mobile User Identifier (TMUI) as described in existing cellular standards. The generation of per-call encryption keys can be carried out using the authentication key using procedures described in existing cellular standards.

In other words, the airlink security procedures in existing cellular standards can be used without modification after the generation of the authentication key using the methods described here.

Industrial Application

My invention is capable of exploitation in industry, and can be made and used, whenever is it desired to register a wireless subscription in a new wireless terminal. The individual components of the apparatus and method shown herein, taken separate and apart from one another, may be entirely conventional, it being their combination which I claim as my invention.

While I have described various modes of apparatus and method, the true spirit and scope of my invention are not limited thereto, but are limited only by the following claims and their equivalents, and I claim such as my invention.

CLAIMS

1) A method for registering a wireless subscription to a wireless terminal, the method comprising the steps of:

a) entering a user identifier) and a password) into the wireless terminal;

b) at the wireless terminal:

i) generating a public/private key pair;

ii) using the password to encrypt the wireless terminal's public key according to a secure key exchange (SKE) protocol, thereby forming a first SKE message; and

iii) transmitting the user identifier and the first SKE message to a home system;

c) at the home system:

i) generating a public/private key pair;

ii) using the user identifier to determine the password;

iii) using the password to encrypt the home system's public key according to an SKE protocol, thereby forming a second SKE message;

iv) transmitting the second SKE message to the wireless terminal;

v) using the password to decrypt the wireless terminal's public key; and

vi) using the home system's private key and the wireless terminal's public key to form a session key;

d) at the wireless terminal:

i) using the password to decrypt the home system's public key; and

ii) using the wireless terminal's private key and the home system's public key to form the session key; and

e) at both the wireless terminal and at the home system, using the session key todownload all or part of a Virtual User Identification Module (VUIM) from the home system to the wireless terminal.

2) The method of Claim 1, further comprising the step of encrypting the user identifier before transmitting it.

3) The method of Claim 1, further comprising the step of opening a communications channel before transmitting the second SKE message to the wireless terminal.

4) The method of Claim 1, wherein the steps of transmitting the SKE messages from a source to a destination further comprise the steps of:
   a) transmitting the SKE messages from the source to an intermediate serving system; and
   b) transmitting the SKE messages from the intermediate serving system to the destination.

5) The method of Claim 4, further comprising the steps of:
   a) using a first portion of the session key as an authentication key in subsequent authentications of the wireless terminal in the intermediate serving system; and
   b) using a second portion of the session key as an encryption key in subsequent control signal transmissions.

6) The method of Claim 1, wherein:
   a) the public/private key pairs comprise Diffie-Hellman public/private key pairs; and
   b) the SKE messages comprise Diffie-Hellman Encrypted Key Exchange (DH-EKE) messages.

7) The method of claim 1, wherein:
   a) the step of using the password to encrypt the wireless terminal's public key comprises the steps of:
      i) first concatenating the wireless terminal's public key with a first random number, thereby forming a first concatenated number; and
      ii) using the password to encrypt the first concatenated number; and
   b) the step of using the password to encrypt the home system's public key comprises the steps of:
      i) first concatenating the home system's public key with a second random number, thereby forming a second concatenated number; and
      ii) using the password to encrypt the second concatenated number.

8) Apparatus for registering a wireless subscription to a wireless terminal, the apparatus comprising:

a) means for entering a user identifier and a password into the wireless terminal;

b) at the wireless terminal:

i) means for generating a public/private key pair;

ii) means for using the password to encrypt the wireless terminal's public key according to a secure key exchange (SKE) protocol, thereby forming a first SKE message; and

iii) means for transmitting the user identifier and the first SKE message to a home system;

c) at the home system:

i) means for generating a public/private key pair;

ii) means for using the user identifier to determine the password;

iii) means for using the password to encrypt the home system's public key according to an SKE protocol, thereby forming a second SKE message;

iv) means for transmitting the second SKE message to the wireless terminal;

v) means for using the password to decrypt the wireless terminal's public key; and

vi) means for using the home system's private key and the wireless terminal's public key to form a session key;

d) at the wireless terminal:

i) means for using the password to decrypt the home system's public key; and

ii) means for using the wireless terminal's private key and the home system's public key to form the session key; and

e) at both the wireless terminal and at the home system, means for using the session key to download all or part of a Virtual User Identification Module (VUIM) from the home system to the wireless terminal.

9) The apparatus of Claim 8, further comprising means for encrypting the user identifier before transmitting it.

10) The apparatus of Claim 8, further comprising means for opening a communications channel before transmitting the second SKE message to the wireless terminal.

11) The apparatus of Claim 8, wherein the means for transmitting the SKE messages from a source to a destination further comprises:
a) means for transmitting the SKE messages from the source to an intermediate serving system; and
b) means for transmitting the SKE messages from the intermediate serving system to the destination.

12) The apparatus of Claim 11, further comprising:
a) means for using a first portion of the session key as an authentication key in subsequent authentications of the wireless terminal in the intermediate serving system; and
b) means for using a second portion of the session key as an encryption key in subsequent control signal transmissions.

13) The apparatus of Claim 8, wherein:
a) the public/private key pairs comprise Diffie-Hellman public/private key pairs; and
b) the SKE messages comprise Diffie-Hellman Encrypted Key Exchange (DH-EKE) messages.

14) The apparatus of claim 8, wherein:
a) the means for using the password to encrypt the wireless terminal's public key comprises:
i) means for first concatenating the wireless terminal's public key with a first random number, thereby forming a first concatenated number; and
ii) means for using the password to encrypt the first concatenated number; and
b) the means for using the password to encrypt the home system's public key comprises:
i) means for first concatenating the home system's public key with a second random number, thereby forming a second concatenated number; and
ii) means for using the password to encrypt the second concatenated number.

15) A wireless terminal constructed to:

a) receive a user identifier and a password into the wireless terminal;

b) generate a public/private key pair;

c) use the password to encrypt the wireless terminal's public key according to a secure key exchange (SKE) protocol, thereby forming an SKE message;

d) transmit the user identifier and the SKE message to a home system;

e) receive an encrypted public key from the home system;

f) use the password to decrypt the encrypted public key from the home system;

g) use the wireless terminal's private key and the home system's public key to form the session key; and

h) use the session key to download all or part of a Virtual User Identification Module (VUIM) from the home system to the wireless terminal.

16) The terminal of Claim 15, further comprising means for encrypting the user identifier before transmitting it.

17) The terminal of Claim 15, further comprising means for opening a communications channel before transmitting the user identifier and the SKE message.

18) The terminal of Claim 15, wherein a portion of the terminal constructed to transmit the SKE messages from a source to a destination further comprises:

a) means for transmitting the SKE messages from the source to an intermediate serving system; and

b) means for transmitting the SKE messages from the intermediate serving system to the destination.

19) The terminal of Claim 18, wherein a portion of the terminal constructed to encrypt the terminal's public key comprises:

a) means for using a first portion of the session key as an authentication key in subsequent authentications of the wireless terminal in the intermediate serving system; and

b) means for using a second portion of the session key as an encryption key in subsequent control signal transmissions.

20) The terminal of Claim 15, wherein:

a) the public/private key pairs comprise Diffie-Hellman public/private key pairs; and

b) the SKE messages comprise Diffie-Hellman Encrypted Key Exchange (DH-EKE) messages.

21) The terminal of claim 15, wherein:

a) a portion of the terminal constructed to use the password to encrypt the wireless terminal's public key comprises:

i) means for first concatenating the wireless terminal's public key with a first random number, thereby forming a first concatenated number; and

ii) means for using the password to encrypt the first concatenated number; and

b) a portion of the terminal constructed to use the password to encrypt the home system's public key comprises:

i) means for first concatenating the home system's public key with a second random number, thereby forming a second concatenated number; and

ii) means for using the password to encrypt the second concatenated number.

22) A home system constructed to:

a) generate a public/private key pair;

b) receive a user identifier and an encrypted public key from a wireless terminal;

c) use the user identifier to determine password;

d) use the password to encrypt the home system's public key according to a secure key exchange (SKE) protocol, thereby forming a SKE message;

e) transmit the SKE message;

f) use the password to decrypt the wireless terminal's public key;

g) use the home system's private key and the wireless terminal's public key to form a session key; and

h) use the session key to download all or part of a Virtual User Identification Module (VUIM) from the home system to the wireless terminal.

23) The system of Claim 22, further comprising means for opening a communications channel before receiving the user identifier.

24) The system of Claim 22, wherein a portion of the system constructed to transmit the SKE messages from a source to a destination further comprises:

a) means for transmitting the SKE messages from the source to an intermediate serving system; and

b) means for transmitting the SKE messages from the intermediate serving system to the destination.

25) The system of Claim 24, further comprising:

a) means for using a first portion of the session key as an authentication key in subsequent authentications of the wireless terminal in the intermediate serving system; and

b) means for using a second portion of the session key as an encryption key in subsequent control signal transmissions.

26) The system of Claim 22, wherein:

a) the public/private key pairs comprise Diffie-Hellman public/private key pairs; and

b) the SKE messages comprise Diffie-Hellman Encrypted Key Exchange (DH-EKE) messages.

27) The system of claim 22, wherein:

a) a portion of the terminal constructed to use the password to encrypt the wireless terminal's public key comprises:

i) means for first concatenating the wireless terminal's public key with a first random number, thereby forming a first concatenated number; and

ii) means for using the password to encrypt the first concatenated number; and

b) a portion of the terminal constructed to use the password to encrypt the home system's public key comprises:

i) means for first concatenating the home system's public key with a second random number, thereby forming a second concatenated number; and

ii) means for using the password to encrypt the second concatenated number.

FIG. 1

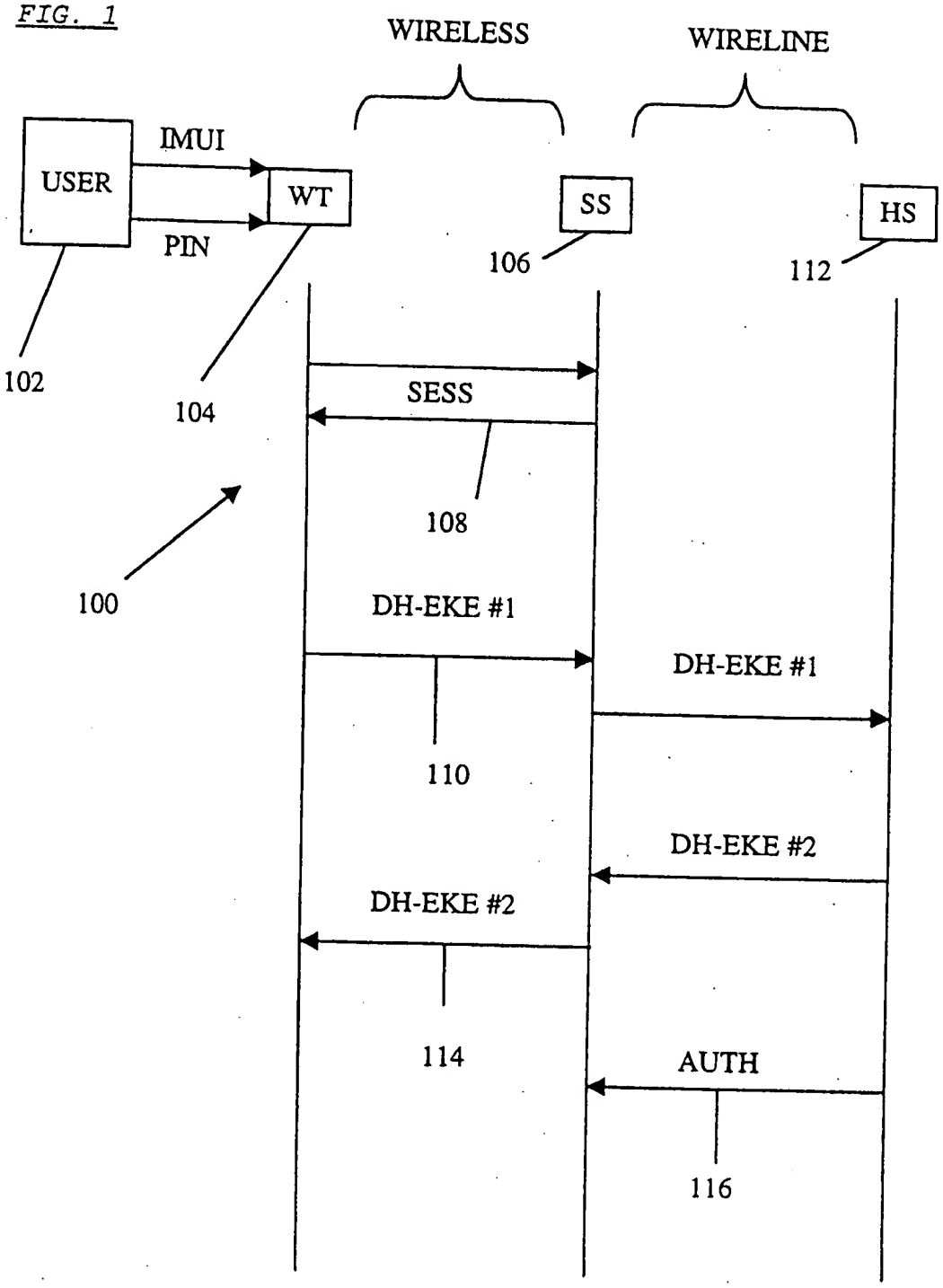
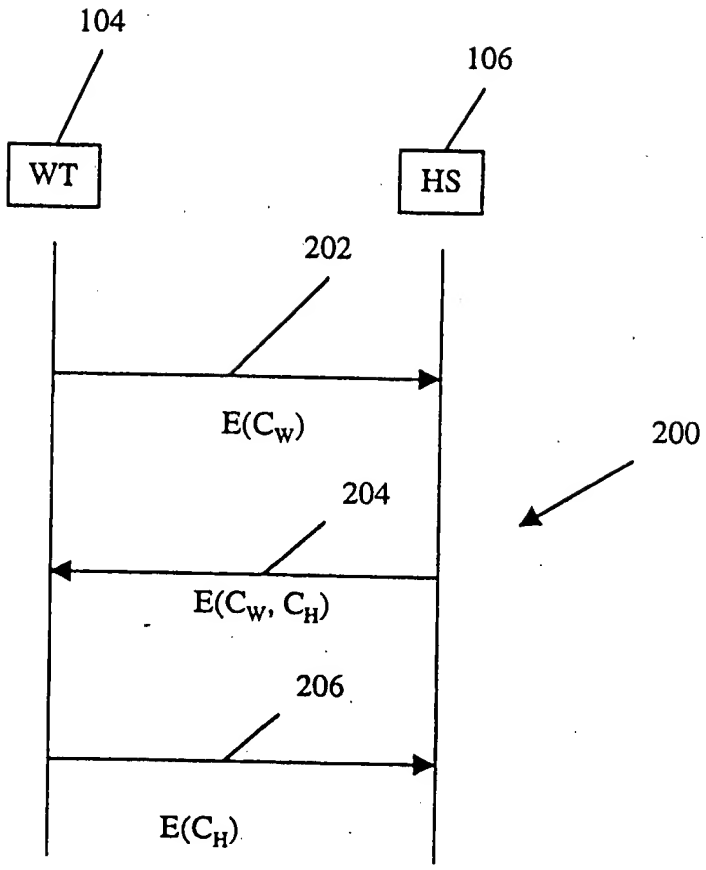

WIRELESS
WIRELINE
USER
IMUI
PIN
WT
SS
HS
106
112
102
104
SESS
108
100
DH-EKE #1
DH-EKE #1
110
DH-EKE #2
DH-EKE #2
114
AUTH
116

FIG. 2



INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/24522

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 535 863 A (AMERICAN TELEPHONE & TELEGRAPH) 7 April 1993 (1993-04-07) page 3, line 44 - line 56 page 4, line 43 -page 5, line 6 page 9, line 11 - line 23 page 11, line 18 -page 12, line 10 figures 1,5,6 --- -/--	1-3,6, 8-10,13, 15-17, 20,22, 23,26

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 February 2000	01/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Barel, C

International Application No
PCT/US 99/24522

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 562 890 A (HUTCHISON MICROTEL LIMITED) 29 September 1993 (1993-09-29) column 1, line 9 - line 56 column 3, line 22 -column 4, line 29 figure 1	1-3,6, 8-10,13, 15-17, 20,22, 23,26
A	EP 0 651 533 A (SUN MICROSYSTEMS INC) 3 May 1995 (1995-05-03) page 5, line 22 - line 49 page 6, line 39 -page 7, line 28 claim 1 figures 4A,4B,4C	1-27
A	TAYLOR A: "OVER-THE-AIR SERVICE PROVISIONING" ANNUAL REVIEW OF COMMUNICATIONS, 1 January 1998 (1998-01-01), XP000793196	

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0535863 A	07-04-1993	US 5241599 A	31-08-1993
		AU 648433 B	21-04-1994
		AU 2351392 A	08-04-1993
		CA 2076252 A,C	03-04-1993
		JP 2599871 B	16-04-1997
		JP 6169306 A	14-06-1994
		NO 923740 A	05-04-1993
EP 0562890 A	29-09-1993	NONE	
EP 0651533 A	03-05-1995	US 5371794 A	06-12-1994
		JP 7193569 A	28-07-1995